Standard Operating Procedure (SOP) for File Shares

Purpose:

This SOP outlines the procedures for creating, managing, and accessing file shares on the company network. It aims to ensure secure and efficient collaboration, data integrity, and regulatory compliance.

Scope:

This SOP applies to all employees who access and share files on the company network.

Responsibilities:

- IT Department:
    - Responsible for setting up and maintaining file shares.
    - Granting access permissions.
    - Monitoring file share usage and activity.
    - Implementing data security measures.
- Employees:
    - Responsible for storing files in designated file shares.
    - Following file naming conventions and folder structures.
    - Granting and managing access permissions for collaborators.
    - Understanding and complying with data security policies.

Procedures:

1. Creating File Shares:

- Contact the IT department to request a new file share.
- Provide a clear description of the purpose and intended users of the file share.
- The IT department will create the file share and set appropriate access permissions.

2. Accessing File Shares:

- Employees will be granted access to file shares based on their job roles and project requirements.
- Access can be granted through individual user accounts or group memberships.
- Employees should use their designated network login credentials to access file shares.

3. File Management:

- Employees must store all work-related files in designated file shares.
- Personal files should be stored on personal devices or designated personal storage areas.
- Follow the established file naming conventions and folder structures to ensure easy organization and retrieval.
- Do not store confidential or sensitive data in non-secure locations like individual desktops.

4. Access Permissions:

- File owners can grant access permissions to other users for collaboration purposes.
- Only grant access to users who have a legitimate need to access the files.
- Different permission levels can be assigned, such as Read, Write, or Modify.
- Revoke access permissions when no longer needed.

5. Data Security:

- Employees must comply with all company data security policies.
- Do not share passwords or access credentials with others.
- Report any suspicious activity or unauthorized access attempts to the IT department immediately.
- Encrypt sensitive data before sharing it outside the company network.

6. Monitoring and Auditing:

- The IT department will monitor file share activity and access logs to ensure compliance and identify potential security risks.
- Regular audits may be conducted to assess file share usage and adherence to SOPs.

Additional Considerations:

- Regularly back up files to prevent data loss.
- Utilize version control systems for collaborative editing of documents.
- Update the SOP regularly to reflect any changes in technology or company policies.